

# Quantum secure communication scheme with W state

Jian Wang,\* Quan Zhang, and Chao-jing Tang  
*School of Electronic Science and Engineering,  
National University of Defense Technology,  
Changsha, 410073, China*

Recently, Cao et al. proposed a new quantum secure direct communication scheme using W state. In their scheme, the error rate introduced by an eavesdropper who takes intercept-resend attack, is only 8.3%. Actually, their scheme is just a quantum key distribution scheme because the communication parties first create a shared key and then encrypt the secret message using one-time pad. We then present a quantum secure communication scheme using three-qubit W state. In our scheme, the error rate is raised to 25% and it is not necessary for the present scheme to use alternative measurement or Bell basis measurement. We also show our scheme is unconditionally secure.

PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) utilizes quantum effects to distribute a secret key among legitimate parties [1, 2, 3]. Different to QKD, Quantum secure direct communication (QSDC) is to transmit the secret message directly without first establishing a key to encrypt them [4, 5, 6]. QSDC can be used in some special environments which has been shown by Boström and Deng et al.[7, 8]. Many researches have been carried out in QSDC [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]. These works can be divided into two kinds, one utilizes single photons, the other utilizes entangled state. Deng et al. proposed a QSDC scheme using batches of single photons which serves as one-time pad [9]. Cai et al. presented a deterministic secure direct communication scheme using single qubit in a mixed state [10]. We proposed a QSDC scheme and a multiparty controlled QSDC scheme using order rearrange of single photons [11]. Einstein-Podolsky-Rosen (EPR) pairs and Greenberger-Horne-Zeilinger (GHZ) states are the main quantum channels exploited in the QSDC. Deng et al. put forward a two-step QSDC protocol using Einstein-Podolsky-Rosen (EPR) pairs [8]. We presented a QSDC scheme using EPR pairs and teleportation [12] and a multiparty controlled QSDC scheme using Greenberger-Horne-Zeilinger (GHZ) states [13]. Wang et al. proposed a QSDC scheme with quantum superdense coding [14] and a multi-step QSDC scheme using GHZ state [15]. Gao et al. and Zhang et al. each presented a QSDC scheme using entanglement swapping [16, 17].

Entanglement is at the heart of quantum information processes. The entanglement of three-qubit is classified by separable, bi-separable, W, and GHZ state [18, 19, 20]. W state has the different physical properties from GHZ state [21, 22]. An important characteristic of three-particle GHZ state is that loss of any one of the qubits leaves the other two in a mixed state with only classical correlations. W state is the 3-qubit state in which each

pair of qubits have the same and maximum amount of bipartite entanglement. This feature makes the entanglement of the W state maximally symmetrically robust against loss of any single qubit. The GHZ class state cannot be transformed to the W class state under any local operation and classical communication (LOCC).

In a recent Letter, Cao et al. proposed a novel QSDC scheme based on a series of four-qubit W states and local Bell basis measurement (hereafter called Cao's scheme) [23]. However, Cao's scheme is not a genuine QSDC scheme. And if an eavesdropper, say Eve performs intercept-resend attack on their scheme, the error rate introduced by her is only 8.3%. Then if the communication parties did not detect the existence of Eve, all the secret messages will be stolen by Eve. To improve the ability of eavesdropping check, we present a quantum secure communication scheme using three-qubit W states. In the present scheme, the error rate introduced by Eve can achieve 25%. At the same time, the efficiency of the scheme is also improved because the communication parties need only to perform deterministic von Neumann measurement. Different to QKD, in our scheme, the communication parties cannot establish a shared key without the sender's measurement results. Only after obtaining the sender's classical message could the receiver recover the sender's secret message, which is different to QSDC in some sort. Therefore we call the present scheme quantum secure communication scheme. The security for the scheme is the same as that for BBM92 protocol [3], which is unconditional secure.

We first consider the intercept-resend attack in Cao's scheme. The four-qubit symmetric W state can be writ-

---

\*Electronic address: jwang@nudt.edu.cn

ten in different bases as

$$\begin{aligned}
|W_4\rangle &= \frac{1}{2}(|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle)_{1234} \\
&= \frac{1}{2}[(|10\rangle + |01\rangle)(|00\rangle + |00\rangle)(|10\rangle + |01\rangle)] \\
&= \frac{1}{2}[|\psi^+\rangle(|\phi^+\rangle + |\phi^-\rangle) + (|\phi^+\rangle + |\phi^-\rangle)|\psi^+\rangle] \\
&= \frac{1}{4}[|++\rangle(2|++\rangle + |+-\rangle + |-+\rangle) \\
&\quad -|--\rangle(2|--\rangle + |+-\rangle + |-+\rangle) \\
&\quad +|+-\rangle(|++\rangle - |--\rangle) \\
&\quad +|-+\rangle(|++\rangle - |--\rangle)], \tag{1}
\end{aligned}$$

where  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ,  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . According to Cao's scheme, Alice sends the  $B$  sequence to Bob. Suppose Eve intercepts the  $B$  sequence and performs  $Z$ -basis ( $|0\rangle$ ,  $|1\rangle$ ) measurement on the two particles  $P_i(3, 4)$  in the  $B$  sequence (In this attack, Eve can also use Bell basis measurement). If Eve's measurement result is  $|00\rangle$  ( $|10\rangle$  or  $|01\rangle$ ), she resends the particles 3, 4 in the state  $|00\rangle$  ( $|\psi^+\rangle$ ) to Bob. In Cao's scheme, Alice will choose randomly  $Z$ -basis,  $X$ -basis ( $|+\rangle$ ,  $|-\rangle$ ) or Bell basis measurement to check eavesdropping. Because of Eve's attack, the  $W$  state collapses to

$$\begin{aligned}
|\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{12}|00\rangle_{34} \\
&= \frac{1}{\sqrt{2}}|\psi^+\rangle_{12}(|\phi^+\rangle + |\phi^-\rangle)_{34} \\
&= \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)_{12}(|++\rangle \\
&\quad +|+-\rangle + |-+\rangle + |--\rangle)_{34} \tag{2}
\end{aligned}$$

or

$$\begin{aligned}
|\Psi_1\rangle &= \frac{1}{\sqrt{2}}|00\rangle_{12}(|10\rangle + |01\rangle)_{34} \\
&= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle)_{12}|\psi^+\rangle_{34} \\
&= \frac{1}{\sqrt{2}}(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle)_{12} \\
&\quad (|++\rangle - |--\rangle)_{34} \tag{3}
\end{aligned}$$

each with probability  $1/2$ . Obviously, Eve's attack will not introduce any error if Alice and Bob perform  $Z$ -basis or Bell basis measurement. If the two parties perform  $X$ -basis measurement, the error rate introduced by Eve will be  $1/4$  according to the Eqs. 1, 2 and 3. Thus the total error rate is  $1/3 \times 1/4 = 0.083$ . And if Alice utilizes this insecure quantum channel to transmit her secret message, according to the process of Cao's scheme, Eve will obtain all of Alice's secret messages because Eve can make certain whether Alice's or Bob's measurement result is  $|\psi^+\rangle$  or  $|\phi^\pm\rangle$  in this attack.

Suppose Alice encodes  $|\psi^+\rangle \rightarrow 0$ ,  $|\phi^\pm\rangle \rightarrow 1$  and Bob encodes  $|\phi^\pm\rangle \rightarrow 0$ ,  $|\psi^+\rangle \rightarrow 1$ . According to Cao's scheme, after the eavesdropping check, Alice and Bob perform Bell

basis measurements on their corresponding particles and they then establish a shared key. The classical messages that Alice sends to Bob are actually the data which Alice generated by using their shared key to encrypt her secret messages. In other words, Alice's outcome encoding  $\oplus$  her secret message equals to classical information, where  $\oplus$  indicates modulo 2 addition. Bob can then recover the secret message by using his outcome encoding  $\oplus$  classical information, which is the same as one-time pad.

We then present a quantum secure communication scheme using three-qubit  $W$  state in order to improve the checking probability and the efficiency for the scheme with  $W$  state. The details of our scheme is as follows:

(S1) Alice prepares  $N$  three-qubit  $W$  states each of which is randomly in one of the two states

$$|\Phi_1\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{123}, \tag{4}$$

$$|\Phi_2\rangle = \frac{1}{\sqrt{3}}(|10+\rangle + |01+\rangle + |00-\rangle)_{123}, \tag{5}$$

where 1, 2 and 3 represent the three particles of  $W$  state. We denotes the ordered  $N$  three-qubit  $W$  states with  $[P_1(1, 2, 3), P_2(1, 2, 3), \dots, P_N(1, 2, 3)]$  (hereafter called  $W$  sequence), where the subscript indicates the order of each three-particle in the sequence. Alice takes the particles 1 and 2 from each state to form an ordered particle sequence  $[P_1(1, 2), P_2(1, 2), \dots, P_N(1, 2)]$ , called  $A$  sequence. The remaining partner particles compose  $B$  sequence,  $[P_1(3), P_2(3), \dots, P_N(3)]$ . Alice selects randomly a sufficiently large subset from the  $W$  sequence for eavesdropping check, called checking sequence ( $C$  sequence). The remaining particles in the  $W$  sequence form a message sequence ( $M$  sequence).

(S2) Alice encodes her secret message on the  $M$  sequence by performing one of the two unitary operations

$$\begin{aligned}
I &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\
U &= i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{6}
\end{aligned}$$

on each of the particles 3 in the  $M$  sequence. If her secret message is "0" ("1"), Alice performs operation  $I$  ( $U$ ). The operation  $U$  flips the state in both  $Z$ -basis and  $X$ -basis, as

$$\begin{aligned}
U|0\rangle &= -|1\rangle, U|1\rangle = |0\rangle, \\
U|+\rangle &= |-\rangle, U|-\rangle = -|+\rangle. \tag{7}
\end{aligned}$$

Alice then sends the  $B$  sequence to Bob.

(S3) After confirming Bob has received the  $B$  sequence, Alice announces publicly the initial states she prepared. If the initial state is  $|\Phi_1\rangle$ , Bob has nothing to do. If the initial state is  $|\Phi_2\rangle$ , he performs Hadamada operation on the particle 3 in the  $B$  sequence.

(S4) Alice publishes the position of the  $C$  sequence. Both Alice and Bob measure the sampling particles in the  $Z$ -basis. Alice let Bob announce his measurement results. If Alice's result is  $|10\rangle$  or  $|01\rangle$  ( $|00\rangle$ ), Bob's result must be  $|0\rangle$  ( $|1\rangle$ ). She can then evaluate the error rate

of the transmission of the  $B$  sequence. If the error rate exceeds the threshold, they abort the scheme. Otherwise, they continue to the next step.

(S5) Alice and Bob perform  $Z$ -basis measurements on their corresponding particles in the  $M$  sequence. Alice then publishes her measurement results of the particles 2, 3 in the  $M$  sequence. Thus Bob can recover Alice's secret message, according to Alice's result, as illustrated in Table 1. Suppose Bob's result is  $|0\rangle$ . If Alice's measure-

TABLE I: The recovery of Alice's secret message

| Alice's result               | Bob's result | secret message |
|------------------------------|--------------|----------------|
| $ 10\rangle$ or $ 01\rangle$ | $ 0\rangle$  | 0              |
| $ 10\rangle$ or $ 01\rangle$ | $ 1\rangle$  | 1              |
| $ 00\rangle$                 | $ 0\rangle$  | 1              |
| $ 00\rangle$                 | $ 1\rangle$  | 0              |

ment result of particle 2, 3 in the  $M$  sequence is  $|00\rangle$  ( $|10\rangle$  or  $|01\rangle$ ), they then conclude that Alice's secret message is "1" ("0").

We now discuss the security for the present scheme. We first consider the intercept-resend attack strategy. In this attack, Eve intercepts the particles in the  $B$  sequence and makes measurements on them. Then she resends a particle sequence to Bob according to her measurement results. In other words, the state of each particle in the resend sequence is equal to her measurement result. Suppose Eve measures the intercepted particle in  $Z$ -basis. If the initial state is  $|\Phi_2\rangle$ , it collapses to  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle+|00\rangle)|0\rangle$  or  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle-|00\rangle)|1\rangle$  each with probability  $1/2$ . Thus the error rate introduced by Eve will be  $1/2 \times 1/3 + 1/2 \times 2/3 = 1/2$ . If the initial state is  $|\Phi_1\rangle$ , Eve's attack will not be detected. In this instance, the total error rate is 25%. Suppose Eve measures the intercepted particle in the  $X$ -basis. Similarly, if the initial state is  $|\Phi_1\rangle$ , the state will collapse to  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle+|00\rangle)|+\rangle$  or  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle-|00\rangle)|-\rangle$  each with probability  $1/2$ . According to the scheme, Bob will perform Hadamada operation on the particle 3. Thus the error rate will also be  $1/4$ . Therefore, in the intercept-resend attack, the total error rate introduced by Eve achieves 25%.

We then consider the collective attack strategy. In this strategy, Eve intercepts the particle  $P_i(3)$  ( $i=1,2,\dots,N$ ) and uses it and her own ancillary particle in the state  $|0\rangle$  to do a CNOT operation (the particle  $P_i(3)$  is the controller, Eve's ancillary particle is the target). Then Eve resends the particle  $P_i(3)$  to Bob. However, Eve cannot make certain the initial state which the particle 3 belongs to. Suppose the initial state is  $|\Phi_1\rangle$ , Eve will

attack successfully. But if the initial state is  $|\Phi_2\rangle$ , the state is changed to

$$|\Phi'_2\rangle = \frac{1}{\sqrt{6}}[(|10\rangle + |01\rangle)(|00\rangle + |11\rangle) + |00\rangle(|00\rangle - |11\rangle)]_{123e}, \quad (8)$$

where the subscript  $e$  indicates Eve's ancillary particle. According to the scheme,  $|\Phi'_2\rangle$  will collapse to  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle+|00\rangle)|00\rangle$  or  $\frac{1}{\sqrt{3}}(|10\rangle+|01\rangle-|00\rangle)|11\rangle$  each with probability  $1/2$ . Similar to the analysis in the intercept-resend attack, in this attack, the total error rate introduced by Eve is also 25%.

In fact, the security for the present scheme is based on entanglement and random Hadamada operation. In the scheme, the random Hadamada operation is equal to selecting  $Z$ -basis or  $X$ -basis randomly to measure the transmitting particle. Note that

$$|\Phi_1\rangle = \frac{1}{\sqrt{3}}[(|10\rangle + |01\rangle)|0\rangle + |00\rangle|1\rangle]_{123}, \quad (9)$$

$$|\Phi_1\rangle = \frac{1}{\sqrt{3}}[(|10\rangle + |01\rangle)|+\rangle + |00\rangle|-\rangle]_{123}. \quad (10)$$

In this way, the security for the scheme is the same as that for BBM92 protocol which is proved to be unconditionally secure. As we described above, our scheme is also unconditionally secure.

So far we have presented a quantum secure communication scheme using W state. The security for the scheme is equal to that for BBM92 protocol. Cao's scheme is not a genuine QSDC scheme because the communication parties first establish a shared key and then encrypt the sender's secret to the receiver. Strictly speaking, our scheme is also not a QSDC scheme because only the sender's measurement result has been published could the receiver recover the sender's secret. Certainly, our scheme is not a QKD scheme because the communication parties can not establish a shared key if the sender's measurement result is not published. Therefore we call the present scheme quantum secure communication scheme. In our scheme, all of the W states are used to transmit the sender's secret message except those chosen for checking eavesdropping. The communication parties need only deterministic von Neumann measurement. In this way, the present scheme is practical within today's technology.

### Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 60472032.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE international Conference on Computers, Systems and*

*signal Processing, Bangalore, India* (IEEE, New York), pp. 175 - 179 (1984).

- [2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [3] C. H. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [4] K. Shimizu and N. Imoto, Phys. Rev. A **60**, 157 (1999).
- [5] K. Shimizu and N. Imoto, Phys. Rev. A **62**, 054303 (2000).
- [6] A. Beige, B.-G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A **101**, 357 (2002).
- [7] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
- [8] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
- [9] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
- [10] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).
- [11] J. Wang, Q. Zhang and C. J. Tang, quant-ph/0603100.
- [12] J. Wang, Q. Zhang and C. J. Tang, quant-ph/0511092.
- [13] J. Wang, Q. Zhang and C. J. Tang, quant-ph/0602166.
- [14] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
- [15] C. Wang, F. G. Deng and G. L. Long, Opt. Commun. **253**, 15 (2005).
- [16] T. Gao, F. L. Yan and Z. X. Wang, quant-ph/0406083.
- [17] Z. J. Zhang and Z. X. Man, quant-ph/040321.
- [18] V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
- [19] W. Dür, G. Vidal and J. I. Cirac Phys. Rev. A **62**, 062314 (2000).
- [20] D. M. Greenberger, M. A. Horne and A. Zeilinger, Am. J. Phys **58**, 1131 (1990).
- [21] J. Joo, Y. J. Park, S. Oh and J. Kim, New J. Phys **5**, 136 (2003).
- [22] P. Walther, K. J. Resch and A. Zeilinger, Phys. Rev. Lett. **94**, 240501 (2005).
- [23] H. J. Cao and H. S. Song, Chin. Phys. Lett. **23**, 290 (2006).